PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-160638
(43)Date of publication of application : 23.06.1995

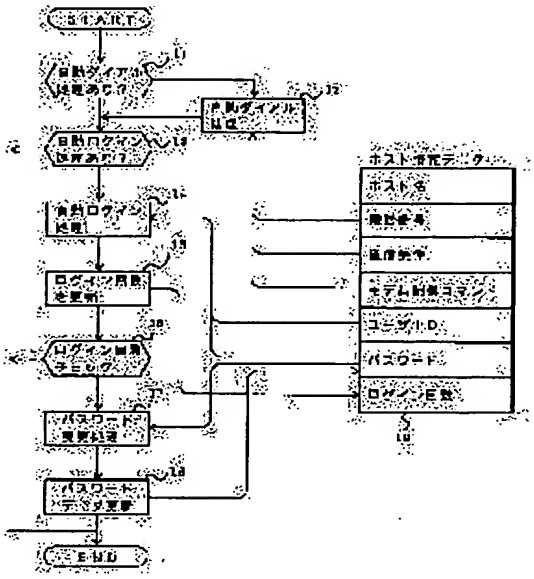
(51)Int.Cl. G06F 15/00

(21)Application number : 05-302513
(22)Date of filing : 02.12.1993

(71)Applicant : HITACHI LTD
(72)Inventor : IIDA TOSHIHIRO

(54) TERMINAL DEVICE FOR INFORMATION EQUIPMENT

(57)Abstract:
PURPOSE: To improve the security in an information equipment network consisting of plural information equipments by occasionally and automatically changing the password data when the log-in procedure is automated to confirm the legitinary of users.
CONSTITUTION: The data are added to the host information data for decision of the password changing timing (19), and these data are checked every time an automatic log-in operation is performed based on the procedure data (15, 16). When the changing of a password is decided, the password of the host side is changed based on the procedure data (17). At the same time, the password of the terminal side is also changed (18). As the passwords are occasionally changed at the terminal side, the security is improved for a terminal device. Furthermore the handling performance of the terminal equipment is also improved since the host information data are also automatically changed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平７－１６０６３８

(43)公開日　平成７年（１９９５）６月２３日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
G06F 15/00	330	B 7459-5L		

審査請求　未請求　請求項の数３　ＯＬ　（全５頁）

(21)出願番号　特願平５－３０２５１３

(22)出願日　平成５年（１９９３）１２月２日

(71)出願人　０００００５１０８
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　飯田　敏裕
茨城県日立市東多賀町一丁目１番１号　株式会社日立製作所情報映像メディア事業部内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】情報機器端末装置

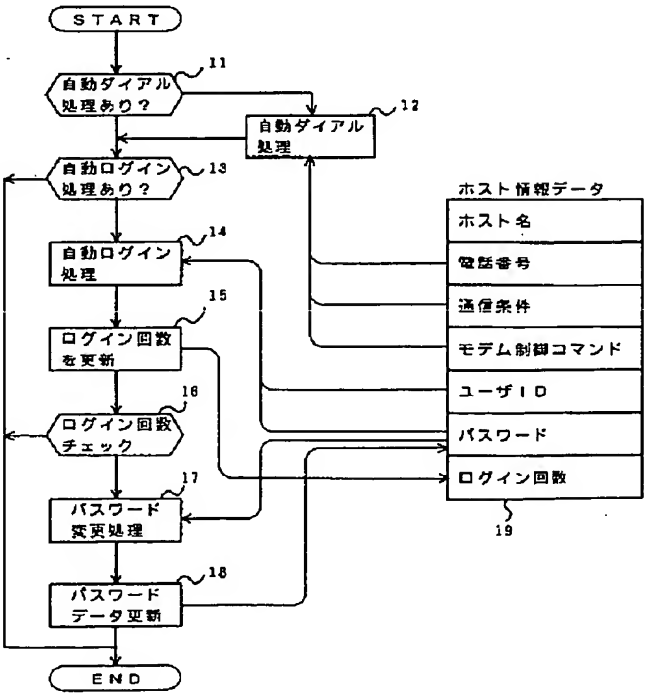
(57)【要約】

【目的】複数台の情報機器から構成される情報機器ネットワークで、利用者の正当性を認証するログイン手順を自動化している場合、パスワードデータを適時、自動的に変更することで、セキュリティを向上させること。

【構成】ホスト情報データに、パスワード変更のタイミングを判断するためのデータを付加し（１９）、手順データを用いて自動ログインするたびに当該データをチェック（１５，１６）して、パスワード変更すると判断した場合に、手順データを用いてホスト側のパスワードを変更する（１７）と共に、端末側のパスワードデータも同時に変更する（１８）。

【効果】端末側で適時パスワードを変更するのでセキュリティが向上すると同時に、ホスト情報データも自動変更されるので使い勝手が向上する効果がある。

図　1



1

【特許請求の範囲】

【請求項１】表示装置／入力装置／記憶装置／通信装置と、それらを制御する制御装置からなる情報機器端末装置において、ユーザＩＤとパスワードを記録可能で、変更可能なホスト情報データと、ホストとの通信を自動化するための、変更可能な通信手順データを具備し、上記データによって使用者の認証処理を自動化した、自動ログイン処理において、

ホスト情報データに、パスワード変更の要否を判断するデータを追加記録して、該データとシステム固有データとを比較することにより、パスワード変更が必要と判断した場合に、予め記録したホスト側のパスワード変更手順を実行すると共に、ホスト情報データ内のパスワードも変更することを特徴とする情報機器端末装置。

【請求項２】請求項１において、パスワード変更の要否を判断するデータとしてログイン回数を記録して、一定回数ごとにパスワードを自動変更することを特徴とする情報機器端末装置。

【請求項３】請求項１において、パスワード変更の要否を判断するデータとしてパスワード変更日時を記録して、一定日数ごとにパスワードを自動変更することを特徴とする情報機器端末装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、複数台の情報機器を接続して運用する場合の、個々の情報機器端末における認証処理に関する。

【０００２】

【従来の技術】複数台の情報機器を接続して運用する、いわゆる情報機器ネットワークは図２のような形態が一般的に用いられる。図２では、ホスト装置（２１）１台、端末装置（２２，２３）２台が、ネットワークケーブル（２４）を介して接続されている。それぞれの装置は、通信装置(２１１，２２１，２３１)，制御装置(212，２２２，２３２)，表示装置（２１３，２２３，２３３），入力装置（２１４，２２.4，２３４）から構成され、ホストには大容量の記憶装置（２１５）も設けられる。この他、プリンタなどの出力装置も設けられるのが一般的だが、特に図示しない。

【０００３】端末がホストの記憶装置等の環境を利用する場合、正当な利用者であるかどうかを判別するため、ログインと呼ばれる認証処理が一般的に行われる（図３）。その際、ユーザＩＤ（利用者の名称）と、パスワードを順に送信し(３１，３２)、正常に認証されればメッセージ等を表示(３３)後、入力待ち状態になる(３４)。通常、端末から送信されるパスワードは、ホストからエコーバック（再送信）されないため、画面には表示されない（３２）。

【０００４】このログイン処理は、図４のように一定のシーケンスで行われるため、ログイン手順を登録して実

2

行したり、図５のように、手順の中からホスト情報データのユーザＩＤとパスワードデータを取り出して実行したりして、自動化するのが一般的である。また、これらのログイン手順やホスト情報データは、端末装置の記憶装置に記録／保持される。

【０００５】

【発明が解決しようとする課題】セキュリティ上、利用者のパスワードは適時変更するのが望ましいとされている。パスワードを変更するには、図６のように、パスワード変更処理を起動し（６１）、古い（現在の）パスワード（６３）と新たなパスワード(６４，６５)を入力しなければならない。

【０００６】このとき、ログイン処理を自動化している場合は、ログアウト後、手順データまたはホスト情報データを手動で変更しておかなければ、次回のログイン処理が正常に行えなくなる。

【０００７】本発明が解決しようとする課題は、このパスワード変更処理を自動化し、セキュリティを向上させることである。

【０００８】

【課題を解決するための手段】第１に、ホスト情報データにパスワード変更のタイミングを判断するデータを追加し、第２に、パスワード変更シーケンス（図７）をログインシーケンス（図４）同様に手順を用いて自動化し、第３に、パスワード自動変更処理からホスト情報データのパスワードを更新する処理を追加する手段を設ける。

【０００９】パスワード変更のタイミングを判断するデータとしては、ログイン回数，パスワードを変更した最終日時などを使用する。

【００１０】

【作用】第１のパスワード変更のタイミングを判断するデータは、ログイン手順内で当該データを参照することによって、パスワード自動変更の要否を判断する。ログイン回数の場合は一定回数ごと、パスワード変更最終日時の場合は最終日時からの経過日が一定期間を過ぎた場合に、パスワード変更要と判断する。第２のパスワード自動変更処理は、第１のデータにより自動変更すると判断した場合に起動される。第３のパスワード更新処理は、第２の処理が正常終了した場合に行われる。

【００１１】

【実施例】本発明による一実施例を図面により説明する。機器装置の構成等については、すでに説明済みであるため省略する。

【００１２】図１は、本発明によるパスワード自動変更処理を含んだログイン処理の概略フローチャートである。

【００１３】まず、自動ダイアル処理（１２）によりホストに接続する。これはネットワークが回線交換により構成される場合のみに実行され、不要な場合はパスされ

る（１１）。不要な場合はホスト情報データ（１９）の電話番号を未設定にするなどして指示する。

【００１４】次に、自動ログイン処理の要否を判断し（１３）、必要なら自動ログイン処理を行う（１４）。自動ログイン処理の要否は、自動ログイン手順が設定されているかどうかで判別する。

【００１５】自動ログイン処理では、ホスト情報データのユーザＩＤとパスワードを利用する。この処理手順は図５に示した通りである。

【００１６】ログインが正常に行われた場合、ホスト情報データのログイン回数データを更新（１加算し記憶装置上のデータを書き換える）する（１５）。ログインが正常に行われたかどうかは、ユーザＩＤ／パスワード入力後のホストからのメッセージで判別可能である。

【００１７】１０回ログインするごとにパスワードを変更する場合は、ログイン回数が１０回に達した場合にパスワード変更処理に分岐する（１６）。この他、１０で割った余りで判断する方法もある。パスワード変更をかける回数はシステム固定でもよいし、ユーザ設定値としてホスト情報データに記録してもよい。

【００１８】パスワード変更処理では、ホスト情報データのパスワードを用いて、図７に示した手順でホスト側パスワードの変更を行う（１７）。新たなパスワードは、図示しないが乱数発生装置を用いて生成することができる。

【００１９】パスワードの変更が正常に行われた場合、ホスト情報データのパスワードを、新しいパスワードデータで置き換える（１８）。

【００２０】図８は、（１７）および（１８）の処理を詳細に記したものである。新しいパスワードデータ（８９）は、生成後からホスト情報データに格納するまで保持される。

【００２１】本実施例によれば、一定回数ログインするごとに、ホスト側と端末側のパスワードデータが同時に変更され、新しいパスワードは乱数により生成されるので盗用されにくい。従ってセキュリティ向上に大きな効果があるとともに、使い勝手が向上する。

【００２２】

【発明の効果】本発明によれば、ホスト側と端末側のパスワードデータが自動的に更新されるので、セキュリティと使い勝手の向上に効果がある。

【図面の簡単な説明】

【図１】本発明による一実施例の、パスワード自動変更付き自動ログイン処理のフローチャートである。

【図２】一般的な情報機器ネットワークの機器構成を示す図である。

【図３】ログイン処理の画面例を示す図である。

【図４】ログイン処理のシーケンスである。

【図５】自動ログインのための処理フローとホスト情報データ構成を示す図である。

【図６】パスワード変更処理の画面例を示す図である。

【図７】パスワード変更処理のシーケンスである。

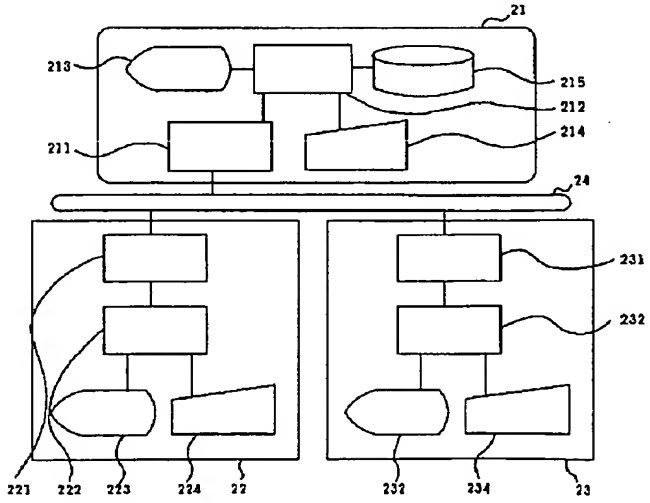
【図８】図１のパスワード自動変更処理の詳細フローとホスト情報データ構成を示す図である。

【符号の説明】

１１，１２…自動ダイアル処理、１３，１４…自動ログイン処理、１５，１６…パスワード変更要否の判断処理、１７，１８…パスワード自動変更処理、１９…ホスト情報データ、２１…ホスト装置、２２，２３…端末装置、２４…ネットワークケーブル、２１１，２２１，２３１…通信装置、２１２，２２２，２３２…制御装置、２１３，２２３，２３３…表示装置、２１４，２２４，２３４…入力装置、２１４…大容量記憶装置。

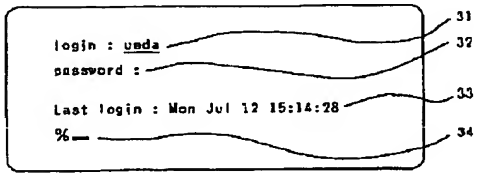
【図２】

図 2



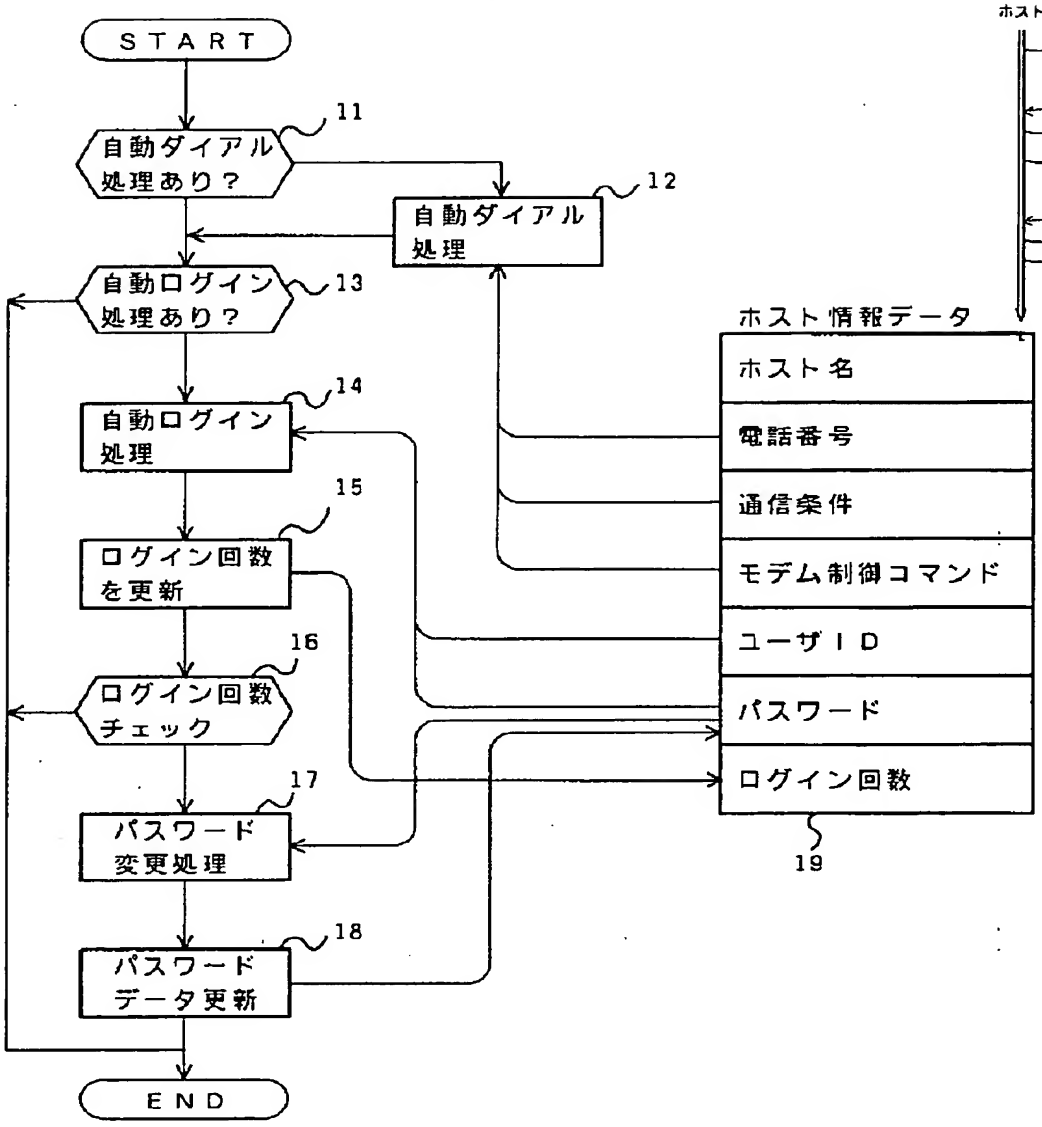
【図３】

図 3



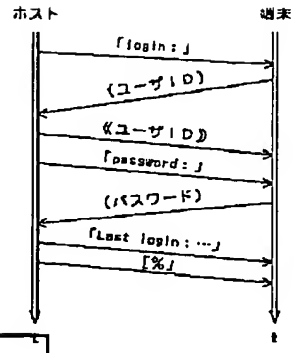
【図１】

図　1



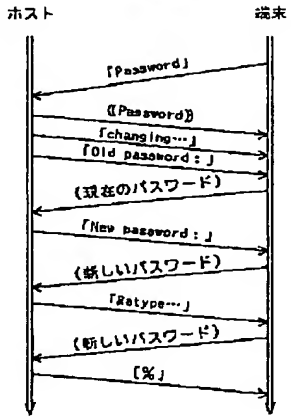
【図４】

図　4



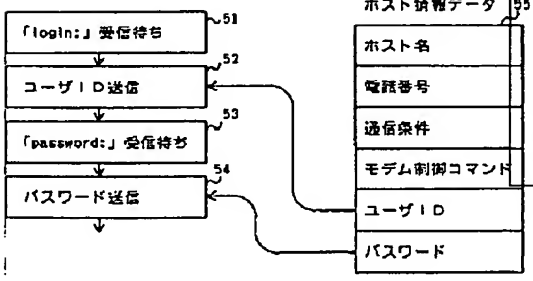
【図７】

図　7



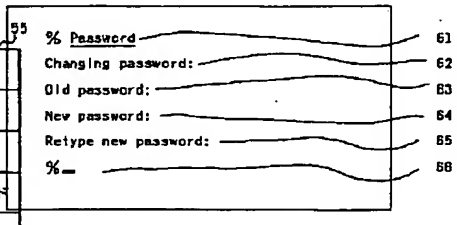
【図５】

図　5



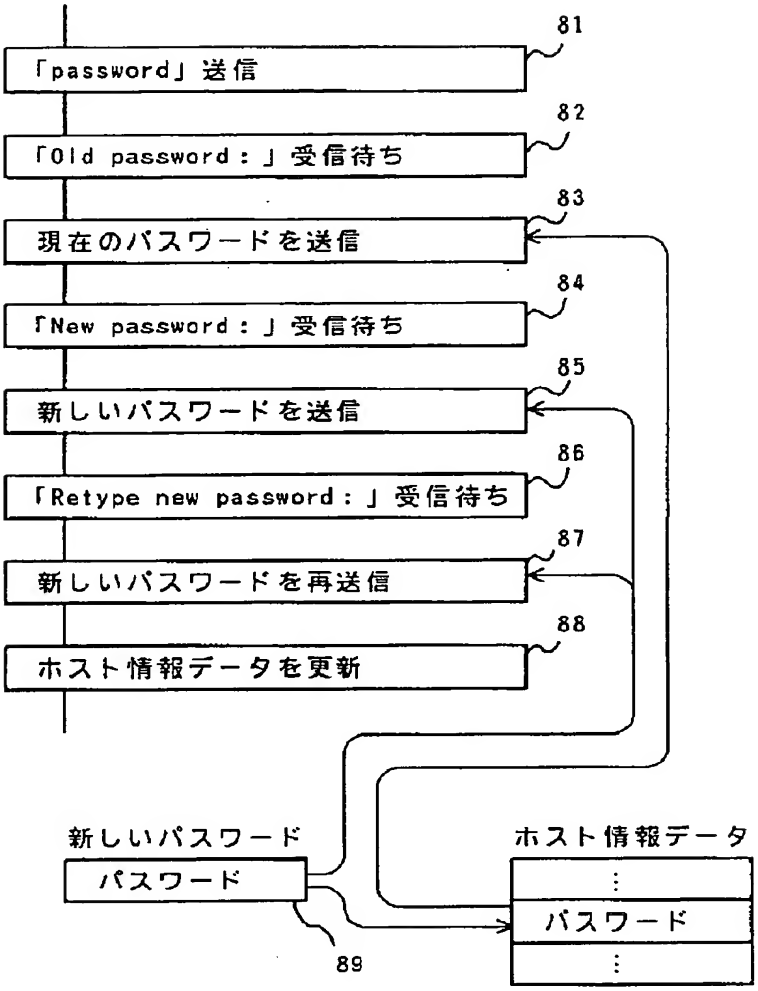
【図６】

図　6



【図８】

図　８


81
「password」送信
82
「Old password：」受信待ち
83
現在のパスワードを送信
84
「New password：」受信待ち
85
新しいパスワードを送信
86
「Retype new password：」受信待ち
87
新しいパスワードを再送信
88
ホスト情報データを更新
新しいパスワード
パスワード
89
ホスト情報データ
パスワード

Our Ref.: OP1710-US

(Prior Art Reference)

Japanese Patent laid-Open Publication No.07-160638

Laid-open Date: June 23, 1995

Title of the Invention: TERMINAL DEVICE FOR INFORMATION EQUIPMENT

Application Number: 05-302513

Date of Filing: December 2, 1993

Applicant: ID No. 000005108

HITACHI LTD

Chiyoda-ku, Tokyo, Japan

Inventor: Toshihiro IIDA

Pertinent Description ([0012]-[0021])

[0012]

Fig. 1 is a schematic flowchart of login processing which includes automatic password changing processing, in accordance with the present invention.

[0013]

First, automatic dialing processing (12) is performed to connect to a host. This is executed only in a case of a network constructed with a circuit switcher, and if this processing is not necessary, it is skipped (11). In this case, instructions are given not to set a telephone number included in host information data (19), etc.

[0014]

Next, a judgment is made as to whether automatic login processing is necessary or not (13). If necessary, then the automatic login processing is performed (14). Whether the automatic login processing is necessary or not is distinguished by whether or not an automatic login sequence has been configured.

[0015]

A user ID and a password serving as host information ID are used in the automatic login processing. This processing sequence is as shown in Fig. 5.

[0016]

When the login has been performed without problems, data indicating a number of login times which is included in the host information data is updated (i.e., the number of login times is increased by 1 and data in a storage device is rewritten) (15). Whether or not the login has been performed without problems can be distinguished by a message from the host after the user ID/password have been inputted.

[0017]

If the password is to be updated every 10 times that the login is performed, then when the number of login times reaches 10, the processing splits off to password alteration processing (16). Alternatively, there is also a method of performing the judgment based on a remainder after dividing by 10. The number of times after which the password is to be changed may be fixed in the system,

or it may also be recorded in the host information data as a value set by the user.

[0018]

In the password alteration processing, the password in the host information data is used to alter the password on the host side according to the sequence shown in Fig. 7 (17). The new password can be generated using a random number generation device which is not shown in the diagram.

[0019]

When the password has been changed without problems, the password in the host information data is rewritten with the new password data (18).

[0020]

Fig. 8 depicts processing (17) and (18) in detail. The new password data (89) is held from the time of generation until storage in the host information data.

[0021]

According to this embodiment, every time the login is performed a given number of times, the password data are simultaneously updated on the host side and on the terminal side, and the new password becomes difficult to steal because it is generated by random numbers. This has a significant effect for improving security, and also improves ease of use.